ARTICLE APPEARED
ON PAGE A17

NEW YORK TIMES
18 March, 1985

Experts Study Effect on La... Of Latest Electronic Services

By DAVID BURNHAM
Special to The New York Times

WASHINGTON, March 17 — A few months ago, Leo Radosta of Detroit pleaded guilty to involvement in a cocaine trafficking ring and was sentenced to 10 years in Federal prison.

For at least two years, Mr. Radosta and 12 of his associates were the subject of a special kind of investigation that raised, but in the end did not answer, a series of complex new questions about the kinds of legal protections that should be extended to information in the computer age.

The questions were raised when a Federal grand jury requested the Source Telecommunications Company, a subsidiary of Reader's Digest, to provide it with "any and all records, writing or documents, including printouts of any and all records, data, documents or electronic mail" about Mr. Radosta, his associates and their companies.

The lack of Federal laws to protect the tens of millions of electronic messages now being transmitted each year by Source Telecommunications and a growing number of other companies offering similar services was the focus of a conference here recently.

The Ethical Use of Computers

The conference was organized by Jerry Berman, an attorney for the American Civil Liberties Union, and by the Public Interest Computer Association to examine the impact of new technologies on the law.

The conference was unusual in that it brought together staff members from a half-dozen Senate and House subcommittees involved in communications law; officials from a number of major corporations, including the American Telephone and Telegraph Company, the International Business Machines Corporation and GTE Telenet, as well as Source Telecommunications, and such leading privacy experts as John Shattuck, a vice president of Harvard University, Allen F. Westin, professor of public law and government at Columbia University, and Ronald Plesser, a Washington lawyer and former general counsel of the now defunct Privacy Protection Study Commission.

The conference was not limited to examining the efforts of law-enforcement agencies to penetrate computerized data bases. Of at least equal concern was the lack of Federal laws to handle individual and corporate snoopers.

Source Telecommunications is a relatively new kind of company that offers more than 37,000 subcribers various electronic information and communication services through its computers and telephone network.

An Electronic Filing Cabinet

One of the services it offers, for example, is a kind of electronic filing cabinet in which a subscriber who has his own personal password may privately store, change or delete information. Other services allow subscribers to exchange electronic messages.

But when attorneys for Source Telecommunications and its customers argued that the electronic messages held by the company were mechanically but not legally under its control, Leonard R. Gilman, the United States Attorney in Detroit, contended in a responding brief that the material requested by the grand jury was not protected by law or judicial rulings that guard a telephone call or letter from examination without a warrant.

The consensus at the conference appeared to be that technology had outgrown existing Federal law and that Congress ought to close the loopholes.

A spokesman for the United States Attorney's office in Detroit said Source Telecommunications provided the grand jury with billing information about the targets. But legal questions about information the company held that belonged to its customers were not resolved, the spokesman said, because the targets were indicted before a judicial decision was handed down.

Electronic mail companies are subject to other kinds of searches, the nature of which makes estimating their actual threat difficult to measure.

In the last few years there have been a number of highly publicized cases in which young computer experts or disgruntled employees or former employees have broken into the computers of private corporations or government agencies.

There are indications, however, that this type of penetration by individuals may be only one aspect of the problem.

Five months ago, for example, Walter G. Deeley, the senior intelligence official responsible for protecting sensitive Government information, charged for the first time publicly that electronic surveillance by the Soviet Union, foreign intelligence agencies and a number of major corporations posed a threat to national security.

And most major oil companies are reported to be so concerned about corporate espionage that they regularly encode seismographical and drilling data transmitted electronically.

A '$100 Million Industry'

Electronic mail companies represented a "$100 million industry," Michael F. Cavanagh, executive director of the Electronic Mail Association, a trade group that represents about 40 major companies, told the conference. He predicted that by the early 1990's the companies would gross at least $1 billion a year.

The participants decided that devising solutions for the industry's legal problems would require both the passage of new laws and amendments to existing laws.

Generally, they appeared to agree on two goals. The first was the passage of laws establishing standards when law-enforcement agencies could appropriately obtain warrants to get information held by electronic mail companies.

The second was adoption of a narrowly worded Federal statute to be used in the prosecution of corporate spies and others who rifled the computer data bases of private companies.